Cued Mnemonics for Better Security and Memorability

Primal Wijesekera, Ivan Cherapau
Department of Electrical and Computer Engineering
University of British Columbia
{primal,icherapau}@ece.ubc.ca

Ayumi Samarakoon
Department of Psychology
University of British Columbia
ayumi3333@gmail.com

Konstantin Beznosov
Department of Electrical and Computer Engineering
University of British Columbia
beznosov@ece.ubc.ca

ABSTRACT

Passwords are still the most used authentication mechanism for wide spectrum of use cases. Memorability and security of human-chosen passwords are two of the most researched areas in authentication. Mnemonics has been widely accepted as a good middle ground between memorability and security. However, it has been shown lately that mnemonics can be vulnerable to carefully crafted dictionary attacks, as more people can converge to smaller set of chosen phrases. We present a novel approach in which, a totally random password is selected first and a text phrase that can act as a mnemonic to the password is generated afterwards. In generating the text phrase, user's background information is used so that text phrase can act as a cue/marker that triggers the memory hence better text recalling. We believe such an approach will both increase security and memorability of textual passwords.

Categories and Subject Descriptors

K.6.5 [**MANAGEMENT OF COMPUTING AND INFORMATION SYSTEMS**]: Security and Protection, Authentication; H.1.2 [**Models and Principles**]: User/ Machine Systems, Human Factors

General Terms

Security, Human factors

Keywords

Mnemonic phrases, password selection

1. INTRODUCTION

Passwords based on mnemonic phrases are believed to reach the common grounds between memorability and security of human chosen passwords. We refer to the passwords based on mnemonic phrases as "mnemonic passwords." Memorability refers to the ability of recalling the text and the security refers to the ability of a given password to withstand a dictionary or brute-force search attack. Memorability is important since it increases the usability of the systems and it was previously shown that reduced usability could degrade the overall security [2]. It was also shown that passwords that are not based on mnemonics are harder to memorize compared to mnemonic passwords [9, 2].

Our approach reverses the conventional method of creating mnemonics passwords. Traditional systems for mnemonic passwords ask the user to come up with a phrase, that is easier to memorize. Depending on the password policy being used, the system might force the user to have different classes of characters in the phrase (such as digits, special characters). Finally selected characters from each word compose the password, with the first letter being commonly used. Now the burden of memorizing a random password moves to memorizing the text phrase selected by the user. Since the phrase is selected by the user herself, it helps the user to remember the password more easily, compared to a random system-generated password.

The guessability of the mnemonic passwords entirely depends on the text phrase selected by the user [1]. With the growing number of online users and concurrently active number of accounts, probability of overlapped phrases is getting high which affects the final password. For this reason, it was shown that mnemonic passwords can be vulnerable to specially crafted dictionary attacks and encourage users not to stick to common phrases, such as excerpt from films, books and songs [3].

We propose a mechanism where guessability of system-generated passwords is preserved while the memorability is improved. Our approach is the exact opposite of what is being done right now. The user is first given a random password and then a mnemonic phrase is generated. The key idea here is to come up with a way of producing such a mnemonic phrase that both allows reproducing the password and is relatively easy to recall. To come up with a phrase that triggers the recall, user's publicly available data, such as her profile(s) and posts in popular social networks can be used. Alternatively, the system can specifically ask the user to enter information that can be later used to compile the mnemonic phrase.

2. PSYCHOLOGY IN TEXT RECALLING

Studies on episodic memory suggest that humans have better recall for words that trigger certain autobiographical episodes that an individual may have experienced. Personal memories are used as "landmarks" that allow the individual to more easily and efficiently recall certain personal experiences [7]. In the same way, people remember information better when it is related to them, which is a cognitive process called the "self reference effect": when individuals produce cues for retrieval, the more cues are related to them the more salient they are. This is the reason people often use biographical information for their passwords (e.g., birthdates), but these are generally weak because they can be easily guessed.

User	Interests	Random Password
User 1	Cricket, Baseball	BRit1ic&DBitbib
User 2	Apple	wSw25hnww$100m
User 3	Skateboarding, Skiing	Wimfpfws!

Table 1: User Interests and Random Passwords

Another process known as the generation effect is the idea that self generated words are better remembered than words presented to the individual. Slamecka and Graf [6] found in their research that participants had higher recall for words they had generated themselves compared to words they were presented with. Memory can also be further enhanced through the method of chunking (Nelson-Vu, 2010). This involves the individual actively incorporating information into chunks therefore creating units to be processed into their memory rather than individual components. This strategy works due to the individual reducing the number of items that need to be stored into their memory, but this chunking of information must be done in a meaningful manner (Vu et al., 2007). A study conducted by Vu et al. showed that participants that randomly incorporated numbers and characters together in a password did not have high recall results compared to participants who placed numbers and characters in meaningful manner that was relevant to them.

The dual coding theory posits that there are explicit differences when encoding verbal information and images into memory. Studies have shown that people have higher recall for images, compared to verbal information, which is a finding that was termed the picture superiority effect. However there are well known vulnerabilities in graphic passwords, such as shoulder surfing attack [4].

3. APPROACH

As suggested by Tulving [7], self reference effect is going to be vital in creating the mnemonic phrase for the password. The key question to answer here is how to generate a text phrase that works as a mnemonic for a given password and is also personally related. The more personally-related it is, the more it helps the user to memorize the phrase, thus increasing the usability and avoiding unwanted affects. Table 1 shows the randomly generated password and the interests shown by the user. These interests can be obtained through publicly available information or directly from the user. As the system evolves, a knowledge base can be created for each user, which can then be used in future password generations. The knowledge base can include information like user's interests, bio, hobbies, etc. This could be a third party single sign-on system providing the service of phrase generation or each system can manage their own knowledge base for the users.

Table 2 shows what could be a personally-related text phrase that can also work as a cue for the password. The key point here is that all the text phrases are personally related to the given user, such as biographical information. And, at the same time, they are different from one password to another, since they are randomly generated. This eliminates any future vulnerability that could arise due to many people using a small set of publicly available phrases for creating mnemonic passwords, leading to easily guessable passwords.

One can also imagine getting information about the user accessible publicly, e.g., on the web, or accessing data from

User	Text Phrase
User 1	Bobby Ruth is top 1 in cricket and Don Bradman is the best in baseball
User 2	when Steve was 25 his net worth was $100 million
User 3	Whistler is my favorite place for winter sports!

Table 2: Sample Text Phrases

places such as Facebook, with the consent of the user. Coming up with words and making a meaningful sentence is already proven in areas, such as Semantic Computing, using ontology and in natural language processing. The proposed knowledge base could be represented in ontologies [8] to store rich domain information gathered from the user. These ontologies can be used to generate words resembling the random password. Techniques in NLP [5] can then be used to generate a meaningful sentence from the words in the knowledge base.

An interesting extension would be to employ the generation effect [6] in the process, to further enhance the memorability. This can be done by letting the user to have more control in generating the phrase. System can present the user with multiple choices for words in the mnemonic phrases. However, this would have other complications on coming up with a meaningful sentence.

4. CONCLUSION

We present a new approach of creating mnemonic passwords by reversing the currently established process. We propose to go from a random password to an easy-to-memorize text phrase. This eliminates a possible vulnerability of using a small set of public phrases and also increases user memorability by making those phrase as cues/markers for triggering the memory. The key question is how to generate a mnemonic phrase by using publicly available data for a given random password.

5. REFERENCES

[1] J. Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 538–552. IEEE, 2012.

[2] P. Inglesant, M. A. Sasse, D. Chadwick, and L. L. Shi. Expressions of expertness: the virtuous circle of natural language for access control policy specification. In *SOUPS '08: Proceedings of the 4th symposium on Usable privacy and security*, pages 77–88, New York, NY, USA, 2008. ACM.

[3] C. Kuo, A. Perrig, and J. Walker. Designing an evaluation method for security user interfaces: lessons from studying secure wireless network configuration. *interactions*, 13(3):28–31, 2006.

[4] A. H. Lashkari, S. Farmand, D. Zakaria, O. Bin, D. Saleh, et al. Shoulder surfing attack in graphical password authentication. *arXiv preprint arXiv:0912.0951*, 2009.

[5] N. Nicolov, C. Mellish, and G. Ritchie. *Sentence generation from conceptual graphs*. Springer, 1995.

[6] N. J. Slamecka and P. Graf. The generation effect: Delineation of a phenomenon. *Journal of experimental*

Psychology: Human learning and Memory, 4(6):592, 1978.

[7] E. Tulving. Episodic and semantic memory 1. *Organization of Memory. London: Academic*, 381:e402, 1972.

[8] M. Uschold and M. Gruninger. Ontologies: Principles, methods and applications. *The knowledge engineering review*, 11(02):93–136, 1996.

[9] J. Yan, A. Blackwell, R. Anderson, and A. Grant. The memorability and security of passwords: some empirical results. *Technical Report-University Of Cambridge Computer Laboratory*, page 1, 2000.